

Procurement and Contracts
900 SW Jackson, Room 102N
Topeka, KS 66612-1286



Phone: (785) 296-2376
Fax: (785) 296-7240
chris.howe@da.ks.gov
www.da.ks.gov/purch

Dennis R. Taylor, Secretary
Chris Howe, Director

Sam Brownback, Governor

AMENDMENT

Amendment Date: November 24, 2007

Amendment Number: 1

Contract ID: 10084

Procurement Officer: Constance S Schuessler
Telephone: 785/296-1171
E-Mail Address: connie.schuessler@da.ks.gov
Web Address: <http://da.ks.gov/purch>

Item: Hospitalization Utilization Review Services

Agency / Business Unit: Kansas Health Policy Authority

Period of Contract: July 1, 2007 through June 30, 2012
With five (5) additional one (1) year periods

Contractor: KANSAS FOUNDATION FOR MEDICAL
2947 SW WANAMAKER DR STE A
TOPEKA KS 66614-4193

Toll Free Telephone: 800-432-0770
Telephone: 785-273-2552
Fax: 785-273-5130
FEIN: 48-0813222
SMART Vendor ID: 0000049303
Contact Person: Larry W. Pittman
lpitman@kfmc.org

Conditions:

Amendment One is executed and on file in Procurement and Contracts. The amendment changes the scope to account for Social Security Administration requirements for using data provided.

Procurement and Contracts
900 SW Jackson, Room 102N
Topeka, KS 66612-1286



Phone: (785) 296-2376
Fax: (785) 296-7240
chris.howe@da.ks.gov
www.da.ks.gov/purch

Dennis R. Taylor, Secretary
Chris Howe, Director

Sam Brownback, Governor

CONTRACT AWARD

Date of Award: June 6, 2007

Contract Number: 10084

PR Number: 014101

Replaces Contract: 30363

Procurement Officer: Beth Schafer
Telephone: 785-296-3122
E-Mail Address: beth.schafer@da.ks.gov
Web Address: <http://da.ks.gov/purch>

Item: Hospital Utilization Review Services

Agency: Kansas Health Policy Authority
Location(s): Topeka, Kansas

Period of Contract: July 1, 2007 through June 30, 2012
With five (5) additional one (1) year periods

Contractor: Kansas Foundation for Medical Care, Inc.
2947 SW Wanamaker Drive
Topeka, Kansas 66614
Toll Free Telephone: 800-432-0770
Telephone: 785-273-2552
Fax: 785-273-5130
FEIN: 48-0813222

Contact Person: Larry W. Pittman
lpitman@kfmc.org

Prices: See Attached

Payment Terms: Net 30

Political Subdivisions: Pricing is not available to the political subdivisions of the State of Kansas.

Procurement Cards: Agencies may not use State of Kansas Business Procurement Card for purchases from this contract.

Administrative Fee: No Administrative Fee will be assessed against purchases from this contract.

CONTRACT AMENDMENT ONE

**FOR UTILIZATION REVIEWS OF SERVICES PROVIDED TO TITLE XIX
BENEFICIARIES
BY HOSPITALS PARTICIPATING IN KANSAS TITLE XIX PROGRAMS
WITH THE
KANSAS FOUNDATION FOR MEDICAL CARE, INC.**

The above referenced agreement was entered into by and between the Kansas Health Policy Authority, hereinafter referred to as "KHPA" and the Kansas Foundation for Medical Care, Inc., hereinafter referred to as "KFMC."

The original contract entered into by KFMC and KHPA providing for inpatient hospital reviews is hereby amended by agreement of the parties.

The Social Security Administration (SSA) has promulgated new requirements regarding access to Personally Identifiable Information (PII) for using such data provided by the SSA. One of these requirements is that the State Agency will undertake in its contractual relationship with each contractor/agent to obtain the contractor's written agreement that the contractor/agent will abide by all relevant Federal laws and access, disclosure and use restrictions, and security requirements in this agreement. The State Agency will provide the contractor/agent with a copy of this agreement and the related attachments before the initial disclosure of data to the contractor/agent. KHPA has determined it is in the best interests of the State to make certain changes to the contract originally agreed upon and to include its agreement with SSA as part of this contract; and KFMC is agreeable to such changes; now for and in consideration of the mutual covenants and agreements contained herein, the parties hereby agree as follows:

1. Personal Identification Information (PII) Confidentiality and Security:

Personal Identification Information obtained from the Social Security Administration (SSA) or with an indication or identifier that the PII has been verified by the SSA is subject to the following requirements:

A. The purpose of this section is to establish terms, conditions and safeguards under which the vendor will, acting as the state's agent, be able to use information relating to the eligibility for, and payment of, Social Security benefits and/or Supplemental Security Income (SSI) and Special Veterans Benefits (SVB), including certain tax return information as authorized by 26 U.S.C. § 6103, released by the Social Security Administration (SSA) to the Kansas Health Policy Authority, hereinafter referred to as the KHPA, for use in:

- 1) Verifying income and eligibility factors for State-administered programs authorized by sections 453 and 1137 of the Social Security Act;
- 2) Verifying Social Security numbers (SSNs) of applicants for, and recipients of, benefits under such programs; and
- 3) Defining safeguards against unauthorized use and redisclosure of such information by the State Agency and its vendor.

This section also establishes the terms, conditions and safeguards under which information relating to the eligibility for, and payment of, Social Security benefits and/or SSI and SVB, for use in State-administered program(s) that are a

SSA under a Federal benefit program and there is a high degree of confidence in the accuracy of the data. The KHPA and its agent(s) may use the above-specified data without independent verification in their administration of the program(s).

b. Opportunity to Contest

The KHPA and its agent(s) agree that there can be no termination, suspension, reduction, final denial, or other adverse action taken against an individual based on this computer match with SSA until there is an opportunity to contest the match information such that:

- (1) Notice is provided by the KHPA and its agent(s) to the affected individual who informs that individual of the match findings and the opportunity to contest these findings.
- (2) The affected individual is given until the expiration of any time period established for the relevant benefit program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond.
- (3) The notice clearly states that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the match data provided by SSA is correct and will make the necessary adjustment to the individual's payment.

E. Procedures for Retention and Timely Destruction of Identifiable Records (5 U.S.C. § 552a(o)(1)(F))

a. State Agency

The KHPA and its agents will retain all identifiable records received from SSA only for the period of time required for any processing related to the matching program and will then destroy the records.

As part of the matching program, any accretions, deletions, or changes to SSA's program rolls provided by SSA to the KHPA and its agent(s) can be used by the KHPA to update its master files, which will be permanently retained under cognizable authority governing the State Agency's retention of records. Any other identifiable records must be destroyed unless the information has to be retained in individual file folders in order to meet evidentiary requirements. In the latter instance, the State Agency will retire identifiable records in accordance with the KHPA records retention policies.

- b. Neither SSA nor the State Agency will create a separate file or system concerning only individuals whose records are used in this matching program.

- d. KHPA and its agent(s) agree to inform personnel including contractors/agents of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.

G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information (PII)

- a. KHPA and its Agent(s):
 - (1) The KHPA and its agent(s) will ensure that all employees and sub-contractors/agents properly safeguard PII furnished by SSA under this agreement from loss, theft or inadvertent disclosure.
 - (2) The KHPA and its agent(s) will ensure that all employees and sub-contractors/agents understand that they are responsible for safeguarding this information at all times, regardless of whether or not the employee or the sub-contractor/agent is at his or her regular duty station.
 - (3) The KHPA and its agent(s) will ensure that laptops and other electronic devices/media containing PII and used by employee and sub-contractors/agents are encrypted and/or password protected.
 - (4) The KHPA and its agent(s) will ensure that when it and/or its sub-contractors/agents are sending email containing PII, all employees and/or sub-contractors/agents do so only from and to addresses that are secure.
 - (5) The KHPA and its agent(s) will ensure that all employees and sub-contractors/agents working under this agreement adhere to the procedures listed in this agreement.
 - (6) The KHPA and its agent(s) will ensure that all employees or sub-contractors/agents limit disclosure of the information and details relating to a PII loss only to those with a need to know.
 - (7) The KHPA and its agent(s) will establish procedures to ensure that when a KHPA employee or contractor/agent employee becomes aware of the possible or suspected loss of PII, the KHPA Systems Security Issues contact:

KHPA Security Officer
Kansas Health Policy Authority
900 S.W. Jackson Street, Room 900-N
Topeka, Kansas 66612-1220
Phone: (785) 296-3981
Fax: (785) 296-4813

is immediately notified of the incident.

When reporting the loss or suspected loss of PII, the report should include the following specific information:

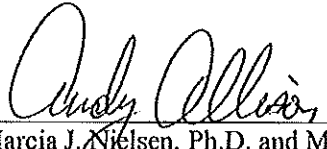
- (a) Contact and component information.
- (b) A description of the loss or suspected loss (e.g., nature of loss, scope, number of files or records and type of

The KHPA will undertake in its contractual relationship with each contractor/agent to obtain the contractor's written agreement that the contractor/agent will abide by all relevant Federal laws and access, disclosure and use restrictions, and security requirements in this agreement. The State Agency will provide the contractor/agent with a copy of this agreement (Attachment 1) and the related attachments before the initial disclosure of data to the contractor/agent.

3. **OTHER:**

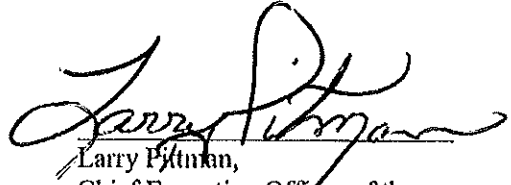
The remaining terms and conditions of the above-referenced original agreement and any attachments and amendments thereto, shall remain in force and effect and binding on the parties hereto.

IN WITNESS HEREOF KFMC and KHPA, hereto affix their signatures to the Amended Contract.

for 

Marcia J. Nielsen, Ph.D. and MPH *org*
Executive Director of the
Kansas Health Policy Authority

10/24/07
Date



Larry Pittman,
Chief Executive Officer of the
Kansas Foundation for Medical Care,
Inc.

10-1-07
Date

I. Purpose

This document provides security guidelines for Federal, State and Local agencies (hereafter referred to as 'outside entity') that obtain information electronically from the Social Security Administration (SSA) through information exchange systems. The guidelines are intended to assist SSA's information exchange partners to understand the criteria SSA will use when evaluating and certifying the system design and security features and protocols used for electronic access to SSA information. The guidelines also will be used as the framework for SSA's compliance review program of its information exchange partners.

II. Role of the SSA Office of Systems Security Operations Management

The SSA Office of Systems Security Operations Management (OSSOM) has agency-wide responsibility for interpreting, developing and implementing security policy; providing security and integrity review requirements for all major SSA systems; managing SSA's fraud monitoring and reporting activities, developing and disseminating training and awareness materials and providing consultation and support for a variety of agency initiatives. OSSOM reviews assure external systems that receive information from SSA are secure and operate in a manner that is consistent with SSA's IT security policies and are in compliance with the terms of information sharing agreements executed by SSA and the outside entity. Within the context of these guidelines, OSSOM conducts periodic compliance reviews of outside entities that use, maintain, transmit or store SSA data in accordance with pertinent Federal requirements to include the following:

- The Federal Information Security Management Act (FISMA)
- Social Security Administration (SSA) policies, standards, procedures and directives.

Correspondence should be sent to:

Director, Office of Systems Security Operations Management
Social Security Administration
Room G-D-10 East High Rise
6401 Security Blvd.
Baltimore, MD 21235

You can also send an email to OSSOM.admin@ssa.gov.

III. General Systems Security Standards

Outside entities that request and receive information from SSA through online, overnight, or periodic batch transmissions must comply with the following general

2. A description of how SSA information will be obtained by and presented to users, including sample computer screen presentation formats and an explanation of whether the system will request information from SSA by means of systems generated or user initiated transactions; and
3. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the outside entity's system and an explanation of their job descriptions.

Meeting this Requirement

Outside entities must explain in their documentation the overall design and security features of their system. During onsite certification and periodic compliance reviews, SSA will use the outside entity's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and compliance reviews and for verifying that the outside entity's systems and procedures conform to SSA requirements.

Following submission to the SSA in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

B. Automated Audit Trail

Outside entities that receive information electronically from SSA are required to maintain an automated audit trail record identifying either the individual user, or the system process, that initiated a request for information from SSA. (Every request for information from SSA should be traceable to the individual or system process that initiated the transaction.) Outside entities that request information from SSA only through batch selection processes from their client data bases need only keep audit trail records identifying the process that generated the transactions forwarded to SSA. However, if such processes are triggered as a result of user requests initiated from the entity's client data base, then the audit trail record must be able to identify the user who initiated the transaction. The audit trail system must be capable of data collection, data retrieval and data storage. At a minimum, individual audit trail records must contain the data needed to associate each query transaction to its initiator and relevant business purpose (i.e. the outside entity's client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored in the audit file as a separate record, not overlaid by subsequent query transactions.

security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The outside entity must have management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the outside entity's system.

Meeting this Requirement

The outside entity must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the administrative function or official responsible for PIN/password issuance and maintenance.

During onsite certification and compliance reviews, the SSA will meet with the individual(s) responsible for these functions to verify their responsibilities in the outside entity's access control process and will observe a demonstration of the procedures for logging onto the outside entity's system and accessing SSA information.

D. Monitoring and Anomaly Detection

The outside entity's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to a legitimate client case (e.g. celebrities, other employees, relatives, etc.) If the outside entity system design is transaction driven (i.e. employees cannot initiate transactions themselves; rather, the system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an employee unless the client system contains a record containing the client's Social Security Number), then the outside entity needs only minimal additional monitoring and anomaly detection. If such designs are used, the outside entity only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the outside entity system by employees not authorized to have access to such information.

If the outside entity design does not include either of the security control features described above, then the outside entity must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual employees,

to monitor user access control violations. The documentation should clearly explain how the system design will prevent outside entity employees from browsing SSA records.

If the outside entity system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an outside entity client), then the outside entity must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA information. The outside entity should include sample report formats demonstrating their capability to produce the types of reports described above. The outside entity should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification and compliance reviews, the SSA will request a demonstration of the outside entity's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the outside entity will demonstrate how the system triggers requests for information from SSA.
- If the design is based on a permission module, the outside entity will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the outside entity system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the outside entity system.)
- If the design is based on systematic and/or managerial monitoring and oversight, the outside entity will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification and periodic compliance reviews, the SSA will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

E. Management Oversight and Quality Assurance

The outside entity must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to

Meeting this Requirement

The outside entity must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The outside entity should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification and periodic compliance reviews, the SSA will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The SSA will also meet with a sample of outside entity employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

G. Data and Communications Security

The outside entity will encrypt all SSN and/or SSN-related information when it is transmitted across dedicated communications circuits between its system, or for intrastate communication among its local office locations. The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

H. SOLQ/SOLQ-I Onsite Systems Security Certification Review

The outside entity must participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the SOLQ/SOLQ-I system. The onsite certification and compliance reviews will address each of the requirements described above and will include, where appropriate, a demonstration of the outside entity's implementation of each requirement. The review will include a walkthrough of the outside entity's data center to observe and document physical security safeguards, a demonstration of the outside entity's implementation of online access to SSA information, and discussions with managers/supervisors. The SSA, or other certifier, also will visit at least one of the outside entity's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.